CRIMES CIBERNÉTICOS: CRIMES DE ALTA TECNOLOGIA

Carina Luna Barbosa - Analista de Sistemas, Bacharela em Direito, estágio na Controladoria Geral da União e Defensoria Pública da Paraíba, pós graduanda em Direito do trabalho e Processo do Trabalho. carinaluna@gmail.com.

RESUMO

O artigo ora apresentado discorre sobre os crimes de alta tecnologia, cujo enfoque é a falta de uma legislação adequada para punição, bem como a informação dos principais crimes. É cada vez maior o número de usuários que usam computadores, fazendo com que a segurança da informação se torne mais vulnerável. Apesar da informática trazer inúmeros benefícios ao ser humano, também traz várias discordâncias, como os crimes contra a honra, crime de invasão de privacidade, pedofilia e fraudes. Devido ao enorme crescimento de redes sociais, os usuários também são responsáveis por alguns desses crimes ao compartilharem pela rede fotos proibidas, encontros para praticar crimes, etc. No ano de 2012 foi sancionada Lei nº 12.737/12, que inseriu alguns artigos ao código penal, porém não foi o suficiente para a quantidade de crimes existentes. Portanto, é necessário propor aos juristas a necessidade da inserção de leis e de estudo mais aprofundado nas faculdades, com a finalidade de aprimorar os estudos jurídicos e adequando-os as tendências mundiais, proporcionando soluções mais coerentes para as questões surgidas no mundo virtual, pois os crimes cibernéticos sempre existirão, mas falta uma legislação mais severa para punir de forma adequada quem pratica tais condutas.

Palavras-Chave: Informática. Segurança. Crimes cibernéticos. Legislação. Punição

Sumário: Introdução. 1 Internet. 1.1 Surgimento da Internet. 1.2 Classificação dos Crimes Virtuais 1.2.1 Crimes Virtuais Próprios 1.2.2 Crimes Virtuais Impróprios. 1.3 Sujeitos dos Crimes. 1.4 Vírus. 2 Crimes de Alta Tecnologia. 2.1 Invasão de Privacidade. 2.2 Crimes Contra a Honra. 2.3 Pornografia Infantil na Internet. 2.4 Crimes contra o Patrimônio. 2.5 Pirataria. 2.6 Falsa Identidade. 2.7 Falsificação de Dados e Cartões. 3 Lei 12.737/12. 4 Competência para julgar os Crimes Cibernéticos. Conclusão. Referências bibliográficas.

Agradeço a Deus e aos meus familiares que sempre ajudaram e estiveram presentes na conquista de mais uma etapa. Agradeço também ao professor que está me orientando neste trabalho pela ajuda e disponibilidade.

INTRODUÇÃO

Diante do crescimento de usuários conectados à rede de Internet, que independente de classes sociais, o fato é que a tecnologia vem trazendo inúmeros benefícios à população, como o acesso à informação, facilidade de estudo com as aulas virtuais, livros etc. Mas não trouxe apenas vantagens, pois aumentou, também, os crimes praticados com o uso da Internet, como, por exemplo: falsificação de dados bancários, invasão de privacidade, pornografia infantil, crimes contra a honra e outros, assim é possível afirmar que esses crimes englobam uma gama muito alta de ataques.

Apesar de existirem publicações sobre como manter a segurança dos dados na Internet, muitos usuários não têm interesse em instalar programas ou aplicativos que dificultam a prática desses crimes que atualmente estão em proporção bastante elevada, tornando quase impossível a punição desses criminosos, seja por uma falta de lei mais severa ou por dificuldade de localizar as pessoas que os cometem. Devido ao enorme crescimento de redes sociais, os internautas são os responsáveis pela maioria desses crimes que não são apenas praticados por crackers. Estes estão qualificados para cometerem abusos cibernéticos que envolvem um nível maior de complexidade, como a mudança de senhas de contas bancárias para transferência entre contas, ou seja, quebra da segurança.

O presente estudo busca um olhar mais detalhado sobre os crimes praticados no meio eletrônico, já que os usuários não aceitam mais que esses crimes sejam praticados sem que se conheça a autoria e sem que haja uma punição adequada pela legislação penal, já que na maioria das vezes é utilizado o Código Penal, considerado antigo, para punir crimes da atualidade, o que deixa uma brecha em relação a punição, pois, na maioria das vezes, não são classificadas como adequadas para as condutas praticadas. Tem como objetivo também mostrar o quanto a legislação brasileira é insuficiente, mesmo sido publicada a Lei nº 12.737/12 que dispõe sobre a tipificação criminal dos delitos informáticos, mas devido à urgência em que ela foi sancionada várias tipificações não foram tratadas. Mesmo com a sanção da referia lei, não houve um consenso sobre a competência jurisdicional referente a esses crimes, uma vez que há divergência na jurisprudência.

1 INTERNET

A Internet é uma rede mundial de computadores que tem em comum um conjunto de protocolos e serviços e seus usuários, quando conectados, têm acesso às informações e comunicações a nível mundial.

1.1 SURGIMENTO DA INTERNET

Teve início no final da década de 60 pelo Departamento de Defesa do Governo Americano cuja intenção era a criação de um mecanismo informatizado de defesa que fosse capaz de resistir a ataques inimigos. Assim, com a destruição de um computador os demais interligados à rede continuariam funcionando normalmente.

Foi desenvolvida pela empresa americana ARPA (Advanced Research Project Agency) na época da Guerra Fria e o sistema recebeu o nome de ARPANET mantendo, assim, a comunicação das bases militares no período da mencionada Guerra. Conforme Wendt Emerson e Barreto Alessandro (2013, p. 79) a Guerra Fria foi o impulso que faltava para a evolução da Internet.

> A Guerra Fria foi o impulso para o início da Internet. Na época, os Estados Unidos pensaram em como colocar vários servidores no ar em pontos espalhados pelo planeta, pois, caso um fosse destruído, os outros não seriam afetados. A grande utilidade disso é que as informações tidas como estratégicas não precisariam ficar armazenadas num ponto só.

Após o fim da ameaça da Guerra o acesso da ARPANET foi liberado aos cientistas, universidades e posteriormente difundido para o uso doméstico quando iniciou-se os crimes eletrônicos.

1.2 CLASSIFICAÇÃO DOS CRIMES VIRTUAIS

Os crimes virtuais podem ser divididos de várias formas, mas, devido à rapidez da evolução dos mesmos, atualmente a classificação que mais se aproxima da realidade é a de crimes virtuais próprios e impróprios.

1.2.1 Crimes Virtuais Próprios

São aqueles cometidos com uso do computador, ou seja, exige, obrigatoriamente, o uso da informática para caracterizar o crime, como por exemplo, a interferência/invasão de dados informatizados, inserção de programas maliciosos com intuito de modificar softwares, hardwares entre outros.

Esse é o pensamento de Damásio de Jesus, citado por Aras (2014)

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado[...].

1.2.2 Crimes Virtuais Impróprios

São aqueles em que o agente faz uso do computador para produzir um resultado como mais um meio para a prática do crime, assim, esses crimes já são tipificados mesmo sem o uso da informática como é o caso da pedofilia.

Entendimento de Damásio de Jesus, citado por Aras (2014)

> Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

1.3 SUJEITOS DOS CRIMES

É difícil comprovar o autor de crimes eletrônicos devido à ausência física do sujeito ativo, por isso houve a necessidade de classificar tais sujeitos de acordo com a especificação de cada um.

1.3.1 Usuários

Os próprios usuários cometem crimes relacionados à informática e algumas vezes agem sem saber que praticam crime, como por exemplo ao postar em redes sociais fotos de terceiros sem a devida autorização, invadindo, portanto, a privacidade daquele. Assim, a frequência com que esses crimes acontecem é muito alta, ficando praticamente impossível sua punição.

1.3.2 Hackers

São pessoas com grandes habilidades em computadores que usam esse conhecimento para melhorar softwares, aplicativos e segurança de sistemas e nunca danificar ou burlar esses sistemas. São pessoas íntegras que, na maioria das vezes, usam a sua habilidade em favor de empresas, sempre agindo eticamente.

Erroneamente têm a fama de criminosos virtuais, mas como já visto são pessoas que atuam aumentando a segurança da informação evitando que os crackers invadam sistemas e usem os dados para prejudicar.

1.3.3 Crackers

Foram criados para serem diferenciados dos hackers já que usam o alto grau de conhecimento que têm em informática com intuito de prejudicar inocentes, assim, são criminosos especializados em invasão da segurança que inserem programas nos dispositivos eletrônicos de terceiros com a intenção de roubar senhas, dados importantes ou simplesmente prejudicar o sistema operacional, fazendo com que o usuário perca todas as informações contidas no computador.

1.3.4 Carder

Pessoas que atuam em grupo ou sozinhas na Internet, cujo objetivo é conseguir dados e senhas de cartões de créditos para realizar fraudes via online. São estelionatários que analisam a vulnerabilidade de usuários que fazem compras via internet extraindo os dados da vítima e realizando compras em outros sites que são entregues em endereços de terceiros, chamados de drops.

Geralmente utilizam softwares próprios para agirem e o mais conhecido é o keylog o qual captura as teclas digitadas no computador.

1.3.5 Wannabes

São pessoas com conhecimento intermediário em informática que querem agir como hackers, porém ainda não têm a competência destes.

1.4 VÍRUS

Vírus são programas instalados nos computadores que infectam o sistema com objetivo de prejudicar desempenho e deixar mais vulnerável a ataques de crackers que roubam dados, senhas e até mesmo números de cartões de crédito. Normalmente vêm em forma de anexo em e-mail, arquivos infectados, ou outras mídias removíveis como pen drives e HD externo. Na maioria das vezes o usuário executa esses arquivos inocentemente, sem fazer ideia que se trata de um programa malicioso.

Para Rafaela Pozzebon (OFICINADANET, 2014) existem outros softwares que agem de forma semelhante aos vírus como, Worm, Spyware, Spam, Phishing, Rootkit etc.

Rafaela Pozzebon (OFICINADANET, 2014) lista dicas de como manter o computador longe das ameaças virtuais, como:

> Utilizar senhas fortes, com letras e números alternados; trocar as senhas periodicamente; usar somente sistemas operacionais atualizados e seguros; sempre ter um bom antivírus atualizado no computador; não abrir anexos desconhecidos em e-mails, ou em mensagens em geral; não baixar arquivos em sites suspeitos; suspeitar sempre de qualquer arquivo enviado.

2 CRIMES DE ALTA TECNOLOGIA

São crimes intencionais normalmente conhecidos como Cibercrimes. Segundo Efraim Turban (2007, p.60, grifo nosso), "[...] são **atividades fraudulentas cometidas com o uso de computadores** e redes de comunicação, particularmente a Internet".

2.1 INVASÃO DE PRIVACIDADE

A Constituição da República Federativa do Brasil em seu artigo 5º, inciso X protege a intimidade, a privacidade, a honra e a imagem das pessoas sendo assegurado a indenização por danos materiais e morais em caso de violação.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

O direito à privacidade não protege apenas o indivíduo atingido, mas sim a coletividade, pois é interesse de toda a sociedade, conforme Marcel Leonardi (2012, p.122)

> [...] não se deve entender a tutela da privacidade como a proteção exclusiva de um indivíduo, mas sim como uma proteção necessária para a manutenção da estrutura social. A privacidade não é valiosa apenas para a vida privada de cada indivíduo, mas também para a vida pública e comunitária [...]

Diante do crescimento de usuários da Internet e a falta de legislação adequada, a invasão da privacidade no mundo virtual vem sendo cada vez maior, pois é de grande dificuldade localizar o local do início da informação e por ser rápido, também o compartilhamento, muitos atos ficam impunes, principalmente se a divulgação ocorreu em países sem legislação específica, assim, o sistema jurídico fica sem efetividade, conforme entendimento de Marcel Leonardi (2012, p.157, grifo nosso) "Se não há uma maneira de saber quem alguém é, onde ele está, nem o que fez ou está fazendo, o sistema jurídico – que é dependente dessas informações para exercer sua força coercitiva – **parece perder sua efetividade**".

Para ter a sua privacidade protegida o usuário deve ficar atento aos sites que visita, aos downloads que faz e, principalmente não abrir e-mails relativos a bancos com cobrança indevida, pois estes não fazem esse tipo de comunicação com seus clientes. Tomando tais atitudes o usuário ficará menos vulnerável a violação de sua privacidade.

2.2 CRIMES CONTRA A HONRA

Previstos no código penal, artigos 138 a 145 que tratam sobre calúnia, difamação e injúria que diferenciam-se apenas quanto à matéria, pois as penas são iguais.

Ocorre o crime de calúnia quando alguém imputar falsamente um fato definido como crime a alguém, conforme artigo 138 do Código Penal "Caluniar alguém, imputando-lhe falsamente fato definido como crime". Esta Conduta é totalmente possível através da Internet. Para identificar tal crime deve-se analisar se a conduta ocorreu através de um site, onde inúmero grupo de pessoas têm acesso, ou através de e-mail direcionado à pessoa ou a um grupo de pessoas. Assim, se a falsa imputação do crime foi realizada através de site ou e-mail com inúmeros destinatários, têm-se configurado a calúnia, porém se foi enviado por e-mail exclusivamente ao ofendido configura a injúria, pois nesse caso somente a honra subjetiva foi atingida.

Esse é o entendimento de Augusto Rossini (2004, p.204) "[...] a publicidade ocorrerá em tudo o que fizer parte, tanto de site quanto de e-mail direcionado a mais de uma pessoa [...]".

A difamação no Artigo 139 do Código Penal é definido como "Difamar alguém, imputando-lhe fato ofensivo à sua reputação". A ofensa é referente à reputação da vítima e não mais um falso crime a ela imputado.

Para Damásio de Jesus (1999, p.217, v.2) na difamação o fato é meramente ofensivo à reputação do ofendido".

Da mesma forma que a calúnia o crime de difamação se consuma pela Internet quando a publicação foi feita a várias pessoas, seja através de sites ou de e-mail com vários destinatários.

No crime de injúria o bem protegido é a honra subjetiva, assim é o sentimento próprio que cada pessoa tem sobre sua honra intelectual ou física.

Segundo Fernando Capez (2012, p.306, v2) "trata-se de um crime de ação livre. Todos os meios hábeis à manifestação do pensamento podem servir à injúria: a palavra oral ou escrita, a pintura, o gesto etc.".

Com esse entendimento é possível que a injúria possa ser praticada em qualquer ambiente da rede, seja por meio de sites ou e-mails, desde que a vítima tome conhecimento. Esse crime não se caracteriza apenas quando a manifestação do preconceito é dirigida à pessoa certa, mas também a grupos de pessoas quando discrimina raça, etnia, religião ou procedência nacional, ou seja, todas as formas previstas no artigo 20, da Lei nº 7716/89, que assim dispõe: "Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. Pena: reclusão de um a três anos e multa".

São crimes motivados pelo preconceito onde o criminoso seleciona suas vítimas por elas pertencerem a um certo grupo diferente do seu. Normalmente está relacionado à raça, à nacionalidade, à regionalidade, à idade, a orientação sexual, ao sexo à deficiência física etc, são comumente chamados de crimes de Ódio.

Não provoca efeitos apenas nas vítimas, mas em todo um grupo aos quais pertencem. Na Internet ocorrem, principalmente, nas redes sociais devido a facilidade de propagação influenciando negativamente uma grande quantidade de pessoas, conforme o site guiadedireitos (2014):

> O Crime de Ódio na Internet é duplamente perigoso. Além de discriminar e tratar de maneira degradante determinados grupos sociais, também incita o preconceito em outros usuários da rede social, especialmente crianças e adolescentes.

2.3 PORNOGRAFIA INFANTIL NA INTERNET**Erro! Indicador não definido.**

Pedofilia é um transtorno sexual que o agente tem e incide em crianças. É muito comum confundir esse transtorno de pedofilia com pornografia infantil, conforme Marcelo Crespo (2011, P.73) "Tecnicamente, pedofilia refere-se a um transtorno da preferência sexual, uma parafilia (um transtorno sexual recorrente), não havendo um crime no Brasil com esta denominação"

Estatuto da criança e do adolescente, Lei 8.069/90, considera criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade.

A legislação brasileira pune diversas situações envolvendo a sexualidade infantil, como a publicação de fotos, vídeos eróticos envolvendo crianças ou adolescentes.

Os crimes que envolvem a pornografia infantil estão no estatuto da criança e adolescente nos artigos 240 e seguintes. "Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente".

A presidenta Dilma Rousseff sancionou O Projeto de Lei (PL) 7.220/2014 que torna Hediondo o crime de exploração sexual da criança, adolescente ou pessoa vulnerável. O projeto estipula como exploração sexual de criança e adolescentes a utilização deles em atividades sexuais remuneradas, a pornografia infantil e a exibição em espetáculos sexuais públicos ou privados. A proposta diz que o crime ocorre mesmo que não haja ato sexual propriamente dito, mas qualquer outra forma de relação sexual ou atividade erótica que implique proximidade física e sexual entre a vítima e o explorador. A pena prevista passa a ser de 4 a 6 anos, inclusive para quem facilitar a prática do crime.

O Fundo das Nações Unidas da Infância criou o aplicativo Projeta Brasil desenvolvido para smartphones que facilita a denúncia para esse tipo de crime, conforme o site projetabrasil (2014).

2.4 CRIMES CONTRA O PATRIMÔNIO

Com o crescimento do uso da Internet os crimes virtuais patrimoniais também aumentaram, e muitos usuários ainda não fazem o uso de softwares que bloqueiam o ataque de

pessoas maliciosas ao seu computador ou outra mídia digital, tendo seus dados revelados a terceiros que os usam de má-fé para obter alguma vantagem.

2.4.1 Estelionato

O crime de estelionato encontra-se definido no artigo 171 do Código Penal "obter para si ou para outrem vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento"

Esse crime configura-se com a obtenção da vantagem ilícita e com o prejuízo alheio, mas o agente deve manter a vítima em erro por meio de algum meio fraudulento (objeto, conversa, sites falsos).

No meio eletrônico, a forma mais usual para cometimento desse crime é através de clonagem de sites ou envio de e-mails falsos que geralmente são referentes a sites de bancos onde o usuário voluntariamente digita seus dados bancários e através da Internet o agente tem acesso a esses dados e os utilizam fazendo a transferência do dinheiro causando prejuízo à vítima. É um crime material que somente se consuma com a obtenção da vantagem ilícita, a não ocorrência do resultado configura a tentativa.

A agência bancária, nesse caso, deve restituir o cliente do dano obtido, pois cabe a agência manter a segurança do seu sistema, tornando a agência bancária o real agente passivo desse crime.

Muitas pessoas confundem o furto mediante fraude com estelionato, porém a Ministra Maria Thereza de Assis Moura, no Acórdão 86.241, **DJ** 20.08.2007 (stj 3ª Seção) esclarece que:

> O furto mediante fraude, escalda ou destreza não se confunde com o estelionato. No primeiro, a fraude visa a diminuir a vigilância da vítima, sem que esta perceba que está sendo desapossada; há discordância expressa ou presumida do titular do direto patrimonial em relação à conduta do agente. No segundo, a fraude visa fazer com que a vítima incida em erro e, espontaneamente, entregue o bem ao agente; o consentimento da vítima integra própria figura delituosa.
> Da análise dos autos, verifica-se que trata de hipótese em que o agente se valeu de fraude eletrônica para transferir R$ 1.530, (um mil, quinhentos e trinta reais) de conta bancária situada em Maringá/PR, por meio da Internt Bankig da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima.
> A fraude, de fato, foi usada par burlar o sistema de proteção e vigilância do Banco sobre os valores mantidos sob sua guarda, configurando, assim, crime de furto qualificado por fraude, não estelionato.
> Considera-se consumado crime de furto no momento em que o agente se torna possuidor da res furtiva, ou seja, no momento em que o bem subtraído sai da esfera de disponibilidade da vítima. No caso em apreço, desapossamento que gerou prejuízo ocorreu em conta corrente situada em Maringá/PR, local da consumação do delito (subtração dares furtiva) prescrito no art. 155, §4º, inciso II, do Código Penal.

Dessa forma, se a conduta teve a utilização de software para capturar senhas bancárias, sites falsos, dispositivo para clonar cartões e os valores são transferidos para contas de terceiros, há o crime de estelionato pois o usuário incidiu em erro, porém se houve a diminuição da vigilância da vítima sem que esta perceba o desapossamento ocorre o crime de furto mediante fraude.

2.4.2 Dano

Crime de dano está definido no artigo 163 do Código Penal "Destruir, inutilizar, ou deteriorar coisa alheia". Assim, dano é um crime possível contra coisas materiais, como computador, impressora, celulares, tablets e outros.

Há vários questionamentos quanto à aplicação desse crime aos danos causados em dados informáticos través de vírus, pois estes dados não se assemelham a coisa já que os dados informáticos não são tidos como materiais.

Devido ao princípio da legalidade que proíbe a utilização da analogia in malam partem em direito penal não é possível caracterizar esse delito como crime de dano.

Esse é o entendimento de Marcelo Crespo (p.59,2011)

> Não há tese capaz de vencer o devido respeito ao princípio da legalidade 164, que proíbe a utilização da analogia in malam partem em direito penal. Portanto, não é possível considerar típico dano a dados informáticos. Dessa forma, caso alguém apagasse dados de um disco rígido (hard disk) sem a autorização do legítimo proprietário, com o exclusivo propósito de lhe causar prejuízo, não se haveria falar de crime de dano, vez que nenhuma "coisa" foi destruída, inutilizada ou deteriorada.
> Não se pode, ao argumento de que se está interpretando extensivamente um conceito, alargá-lo de forma a ultrapassar os limites da legalidade impostos pelo legislador. Em outras palavras, não se pode elevar o termo "coisa material" ao patamar de "coisa imaterial" para incriminações.

Diante da enorme quantidade de dados armazenados em mídias é de fundamental importância uma reforma legislativa inserindo ao artigo 162 do Código penal a expressão dado eletrônico, ficando com a seguinte redação: art. 163 – Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio, conforme projeto de lei 89/03.

2.4.3 Extorsão

O crime de extorsão está tipificado no artigo 158 do Código Penal "Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar fazer alguma coisa"

No meio virtual os agentes para atingirem o que desejam agem retirando do ar o site de uma grande empresa pedindo em seguida resgate para colocá-lo novamente em funcionamento.

Para configurar esse crime deve existir o constrangimento com emprego de violência ou grave ameaça com intuito de obter vantagem econômica. Esse crime, conforme Sumula 96 do STJ consuma-se independentemente da obtenção da vantagem indevida, bastando apenas o constrangimento com a violência ou a grave ameaça.

2.5 PIRATARIA

A Internet trouxe diversas facilidades para os autores, como a divulgação de seus trabalhos e venda dos seus produtos, mas também trouxe complicações, como é o caso da pirataria que é caracterizada pelo download ou distribuição de conteúdo protegido por direito autoral sem a devida autorização ferindo, portanto, o direito à propriedade intelectual. Essa distribuição e downloads são realizados através da rede mediante compartilhamento de arquivos como o torrent que é o compartilhamento de qualquer tipo de arquivo pela Intarnet ou por meio de discos virtuais como o 4shared.

No Brasil a prevenção e a repressão desses ilícitos penais e civis ainda não oferecem condições de defesa adequada da propriedade intelectual.

A Lei nº 9.610/98, que atualiza e consolida a legislação sobre direitos autorais, no seu artigo 26, VI, §3º proíbe o comércio ilegal de obras intelectuais por vias tecnológicas que não tenham autorização legal. Já a Lei nº 10.695/03 adequou o tipo penal artigo 184 do Código Penal que antes tratava apenas de violação do direito do autor, passou a tratar também daquilo que lhes forem conexos, alterou também o Código de Processo Penal estabelecendo o processo do julgamento dos crimes contra a propriedade imaterial.

No ano de 2004 o Decreto Presidencial nº 5.244/04 criou o Conselho Nacional de Combate à Pirataria e Delitos Contra a Propriedade Intelectual cujo objetivo é elaborar diretrizes para o combate à pirataria e à sonegação fiscal dela decorrente.

Para César Bitencourt (P.402, 2014) "Essa previsão legal pode ainda não ser a ideal, mas já se oferece as condições mínimas para se começar a combater a pirataria da era

cibernética". Infelizmente essas alterações não foram suficientes para combater esse crime, pois a falta de uma legislação específica, mais abrangente, faz com que a venda e distribuição de produtos não autorizados seja cada vez maior, causando, inclusive prejuízos aos cofres públicos.

2.6 FALSA IDENTIDADE

Atualmente, com o crescimento das redes sociais, tem sido muito frequente a quantidade de perfis falsos ocultando, assim, a identidade da pessoa.

O Artigo 307 do Código Penal informa que:

> Atribuir a si ou a terceiro falsa identidade para **obter vantagem**, em proveito próprio ou alheio, ou para **causar dano a outros**. Pena: detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

Qualquer pessoa que atribua uma falsa identidade comete esse crime, porém deve existir a intenção de obter vantagem ou causar danos a outrem. O sujeito passivo deve buscar o máximo de provas possíveis, como o Boletim de ocorrência, print da tela com o falso perfil, as ameaças e horário das postagens, bem como os danos que sofreu. Diante dessas provas o delegado abre inquérito, encaminha para o juiz que decide sobre a quebra do sigilo do IP para posterior punição do criminoso.

2.7 FALSIFICAÇÃO DE DADOS E CARTÕES

A utilização de dados de cartões de crédito ou débito obtidos de forma indevida ou sem equipara-se ao crime de falsificação de documento particular, sujeito à reclusão de um a cinco anos e multa.

3 LEI 12.737/12

Essa lei ficou comumente conhecida como Lei Carolina Dieckmann e trouxe algumas alterações ao Código Penal Brasileiro, onde foi tipificado alguns crimes de informática.

Foi através do Projeto de Lei nº 2793/2011 quando a referida atriz teve o seu computador pessoal invadido por crackers que invadiram a sua privacidade e mais de 30 fotos íntimas foram

publicadas na Internet sem qualquer restrição. Devido à grande publicidade que teve esse fato o projeto de Lei foi tramitado com urgência no Congresso Nacional.

Essa lei Inseriu ao Código Penal os artigos 154-A e 154-B sendo estes tipificados como "invasão de dispositivo Informático".

> 154 – A "Invadir **dispositivo informático** alheio, conectado ou não à rede de computadores, mediante **violação indevida de mecanismo de segurança** e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, três meses a um ano, e multa.
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Esse artigo só veio fortalecer o que já era protegido pela Constituição Federal em seu artigo 5º, X que protege a intimidade.

O legislador usou o termo dispositivo informático alheio para que este artigo continuasse sempre atual, assim, não foi taxativo em informar qual o dispositivo é passível de invasão, já que surgem vários tipos de dispositivos informáticos na atualidade.

Por mecanismo de segurança entende-se que são todos os meios capazes de evitar/dificultar a invasão de estranhos ao dispositivo, como login, senha, antivírus, identificação do usuário etc, assim, se alguém usa um dispositivo eletrônico sem mecanismo de segurança e também sem autorização não incorre nesse crime.

Esse é o entendimento de Greco (2014)

> Para que ocorra a infração penal sub examen, exige o tipo penal, ainda, que a conduta seja levada a efeito mediante violação indevida de mecanismo de segurança. Por mecanismos de segurança podemos entender todos os meios que visem garantir que somente determinadas pessoas terão acesso ao dispositivo informático, a exemplo do que ocorre com a utilização de login e senhas que visem identificar e autenticar o usuário, impedindo que terceiros não autorizados tenham acesso às informações nele contidas.

Esse crime é comum, pois qualquer pessoa pode ser sujeito ativo e passivo, inclusive as pessoas jurídicas que podem ter suas informações sigilosas, guardadas em dispositivo informático, invadidas sem a devida autorização.

Esse é o entendimento de Cabette (2013)

> O sujeito passivo da infração é, portanto, qualquer pessoa passível de sofrer dano moral ou material decorrente da ilícita obtenção, adulteração ou destruição de dados ou informações devido à invasão ou violação de seu sistema informático, mediante vulneração de mecanismo de segurança. Assim também é sujeito passivo aquele que sofre a instalação indevida de vulnerabilidades em seu sistema para o fim de obtenção

> de vantagens ilícitas. São exemplos as atuações em que indivíduos inserem vírus espiões para obter, adulterar ou destruir dados em sistemas informáticos.

O tipo subjetivo desse crime é o dolo com o fim de obter ou destruir dados ou informações com a obtenção da vantagem ilícita. Para sua caracterização não há exigência que o dispositivo informático esteja ligado à rede mundial de computadores, protegendo qualquer dado constante no meio virtual.

Essa invasão deve ser sem o consentimento, pois o técnico de informática que quebra o sigilo para consertar o dispositivo tem o consentimento para isso, caso contrário cometeria esse crime.

O caput do artigo 154-A pune quem invade dispositivo informático alheio sem autorização e o parágrafo 1º desse mesmo artigo pune as pessoas que produzem, oferecem, distribuem ou vendem os dados adquiridos com a invasão do dispositivo de informática. § 1º." Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput".

O § 2º aumenta a pena de um sexto a um terço se a invasão do dispositivo informático resultar em prejuízo econômico, que assim dispõe: § 2º "Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico".

Já o § 3º traz as formas qualificadas desse crime prevendo uma pena diferenciada de reclusão de seis meses a dois anos mais multa para os seguintes casos:

I. Quando a invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas – são os e-mails privados, conversas, mensagens, compartilhamento de fotos ou vídeos etc.
II. Quando resultar a obtenção do conteúdo de segredos comerciais ou industriais – são dados de interesses econômicos e negociais que podem ser prejudicados;
III. Quando resultar a obtenção do conteúdo de informações sigilosas, assim definidas em lei – informações protegidas por sigilo legal, normalmente ligados aos órgãos governamentais e à segurança nacional.
IV. Quando resultar o controle remoto não autorizado do dispositivo invadido – relacionado ao acesso remoto clandestino.

O parágrafo 4º informa que as hipóteses do parágrafo 3º têm a pena aumentada de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas. § 4º "Na hipótese do § 3º, aumenta-se a pena de um a dois

terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos".

O parágrafo 5º aumenta a pena de um terço à metade quando esse crime for praticado contra:

I. Presidente da República, governadores e prefeitos;
II. Presidente do Supremo Tribunal Federal;
III. Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
IV. Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Assim, em relação a esse artigo percebe-se que se trata de infração de menor potencial ofensivo, ou seja, aqueles cuja maior pena não ultrapassa dois anos, ficando sujeito à investigação do Juizado Especial Criminal onde a apuração do delito é feita mediante um termo circunstanciado, porém, na maiorias das vezes, esse termo não é suficiente, a que faz-se necessária a investigação pericial, busca e apreensão de equipamentos, oitivas de testemunha, tornando imprescindível a instauração de um inquérito policial.

Já nos casos dos parágrafos 3º e 4º o delito não é mais competente ao juizado especial, pois considerando o aumento de pena esta passa a ser maior que dois anos.

Outra importante alteração que a Lei trouxe para o Código Penal foi a inclusão do artigo 154-B que assim dispõe:

> Art. 154-B Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Por esse artigo entende-se que o crime é de Ação Penal Pública condicionada a representação, pois ofende a intimidade e a vida privada da vítima, mas há exceção quando o crime é praticado contra a administração pública direta ou indireta passando a ser Ação Penal Pública Incondicionada.

A lei 12.737/12 também acrescentou o parágrafo primeiro do artigo 266 do Código Penal que assim dispõe:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento.
> Pena - detenção, de um a três anos, e multa.

> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

Por esse parágrafo primeiro o sujeito comete o crime se interromper o serviço telemático ou de informação impedindo ou dificultando o restabelecimento, porém deixa uma brecha para quem apenas perturba o serviço telemático sem interromper o serviço, onde nesse caso não há punição conforme referido o caput.

Também foi acrescentado o parágrafo único ao artigo 298 do código penal.

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena - reclusão, de um a cinco anos, e multa.
> **Falsificação de cartão**
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

Portanto, foi tipificado o crime de falsificação de cartão, sendo ele de débito ou crédito sem ser necessário especificar qual a instituição financeira o emitiu, caracterizando- o como um instrumento particular.

4 COMPETÊNCIA PARA JULGAR OS CRIMES CIBERNÉTICOS

Por ser a Internet um campo vasto gera muitas dúvidas para julgar os crimes cometidos por meio eletrônico. A jurisdição é um dos maiores problemas relacionados a esses crimes, pois há infinidade de territórios sem leis, o que complica a investigação dos criminosos.

O Brasil, mesmo não tendo uma legislação específica para tais crimes, só pode punir as condutas realizadas nos provedores e usuários situados no país. As ações realizadas em países diversos dificultam a apuração do crime, pois fica dependendo da lei daquele país para que seja iniciada a investigação.

O código Penal brasileiro especifica em seu artigo 5º, parágrafos 1º e 2º sobre a questão da territorialidade da tutela jurisdicional.

> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
> § 1º - Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar.

> § 2º - É também aplicável à lei brasileira os crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em voo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil.

O judiciário sempre resolvia essa questão utilizando a lei de imprensa, Lei 5.250/67, esta informa que a competência é fixada pela teoria da atividade, ou seja, o crime é praticado no momento da conduta.

> Art. 42. Lugar do delito, para a determinação da competência territorial, será aquele em que for impresso o jornal ou periódico, e o do local do estúdio do permissionário ou concessionário do serviço de radiodifusão, bem como o da administração principal da agência noticiosa.

Com a revogação dessa lei o que já era pacificado tornou-se dispensável, pois a Internet teve um crescimento muito rápido, fazendo com que a antiga lei deixasse brechas para alguns crimes.

Diante da falta de legislação, a terceira seção do STJ no julgado Conflito de Competência CC nº 67.343/GO fixou a competência para o local do resultado. Já o TJ/MG julgou que quando o crime é iniciado no Brasil e o resultado no estrangeiro usa-se a teoria da ubiquidade ou mista cuja competência é da Justiça federal.

Assim fica claro que não há unanimidade em relação à competência, principalmente quanto à Justiça Federal e à Estadual e por isso surgiu a PEC nº 407/05 que estipulava a competência como sendo da Justiça federal para os crimes cometidos por meio eletrônico, porém tal proposta fora arquivada no ano de 2007, pois a jurisprudência considerava as razões insuficientes, já que há crimes informáticos simples, que acarretam poucos danos, o que ocasionaria uma sobrecarga à Justiça Federal, devendo ser levados a essa esfera apenas os crimes que lesionem a União ou enquadrados no artigo 109 da Constituição federal.

Portanto deve ser analisado o caso concreto, sendo a Justiça Estadual competente para julgar os crimes eletrônicos que não incluam a União nem os casos do artigo 109 da Constituição federal, caso contrário a competência será da Justiça federal.

Conforme o já citado Acórdão CC 86.241, **DJ** 20.08.2007 (STJ 3ª Seção) página 11 a competência para os crimes de furto ou estelionato no meio eletrônico é o local onde foi realizado a consumação do delito.

CONCLUSÕES

Sobre o trabalho realizado podemos concluir que o uso meio eletrônico associado à Internet vem sendo cada maior, trazendo benefícios e informações à vida dos usuários, mas também vem sendo instrumentos para caracterização de várias condutas tipificadas como crime. A nossa legislação ainda é muito falha em relação a esse assunto, pois na maioria das vezes é utilizado o Código Penal, que por ter uma redação antiga deixa inúmeras brechas para os crimes que não existiam à época de sua criação, como por exemplo, os crimes cibernéticos que vêm aumentando constantemente.

No ano de 20212 foi promulgada a Lei nº 12.737/12, já estudada, porém deixou algumas falhas em seus dispositivos devido a urgência de sua aprovação, não alcançando o seu real objetivo que é a punição dos infratores.

Outra dificuldade também encontrada em relação aos crimes eletrônicos é referente à competência para julgamento desses crimes, uma vez que eles podem ultrapassar as fronteiras do país o que dificulta a investigação, e, por ser um campo fértil, podem surgir vários tipos de delitos. Portanto, como não há uma legislação especificando se a competência é federal ou estadual, juristas vêm afirmando que a competência é da esfera Estadual, mas se os crimes forem cometidos contra a União ou artigo 109 da Constituição Federal a competência passa a ser da esfera Federal.

Por fim, conclui-se que não basta apenas sancionar uma Lei para crimes eletrônicos com grande divulgação na sociedade, mas sim um estudo aprofundado sobre cada crime praticado na Internet, com penas que levem o infrator a pagar pelo delito cometido. Após o estudo deve sim, ser elaborado uma Lei mais rigorosa, sem brechas ou a mudança da tipificação penal alcançando os referidos crimes.

CYBER CRIMES: CRIMES OF HIGH TECHNOLOGY

ABSTRACT

The presented work aims to discuss the high-tech crimes, whose focus is the lack of adequate legislation for punishment as well as information of major crimes. A growing number of users who use computers, make information security becomes more vulnerable. Despite the computer to bring numerous benefits to the human being as consumer relations, contractual, commercial,

etc., also brings several disagreements, such as honor crimes that are extremely common in the Brazilian Internet crime of invasion of privacy, fraud and pedophilia. Due to the tremendous growth of social networks , users are also responsible for some of these crimes prohibited by the network to share photos , dating to commit crimes , etc. , so these crimes are not only committed by attackers. In 2012 was enacted Law Nº 12,737 / 12, which inserted some articles to the Penal Code, but it was not enough for the amount of existing crimes. This work is conducted from a literature search that allowed the analysis of various concepts and doctrines that underlie views on said topic. Therefore, it is necessary to propose the need for lawyers inserting laws and further study in colleges , in order to improve legal studies and adjusting them to global trends , providing more consistent solutions to the issues arising in the virtual world as cyber crimes will always exist , but lack a tougher law to punish appropriately those who practice such behavior

Keywords: Computers. Security. Cybercrimes. Legislation. Punishment

REFERÊNCIAS

ARAS, Vladimir**.** Crimes de informática. Uma nova criminalidade. Jus Navigandi**,** Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/artigos/2250>. Acesso em: 26 out. 2014.

BRASIL. Constituição da República Federativa do Brasil de 1988. Dispõe sobre os Direitos e Deveres Individuais e Coletivos. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 26 set. 2014.

_____. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm>. Acesso em 26 set. 2014

_____. Estatuto da Criança e do adolescente. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 04 out. 2014

_____. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 27 set. 2014

BITENCOURT, Cezar R. **Tratado de Direito Penal**: parte especial 3. 10. ed. São Paulo. Saraiva. 2014.

CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei nº 12.737/12 e o crime de invasão de dispositivo informático. Jus Navigandi, Teresina, ano 18, n. 3493, 23 jan. 2013. Disponível em: <http://jus.com.br/artigos/23522>. Acesso em: 14 out. 2014.

CABETTE, Eduardo Luiz Santos. O novo crime de invasão de dispositivo informático**.** Conjur, 2013. Disponível em: < http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 10/10/2014.

CRESPO, Marcelo X de F. **Crimes Digitais**. São Paulo: Saraiva, 2011.

GUIADEDIREITO. Disponivel em: <http://www.guiadedireitos.org/index.php?option=com_content&view=article&id=1036&Itemid=259> Acesso em: 04 set. 2014

GRECO, Rogério. Comentário sobre o crime de invasão de dispositivo informático art. 154-A do código Penal**.** Disponível em: <http://www.rogeriogreco.com.br/?p=2183>. Acesso em: 17 out. 2014.

JESUS, Damásio E. de. **Direito Penal:** parte especial. 22 ed. Revista e atualizada. São Paulo, Saraiva, 1999, 2v.

LEONARDI, Marcel. **Tutela e privacidade na Internet.** São Paulo: Saraiva, 2012.

NETTO FILHO, Dickson Cirilo Andrade. Crime virtual: crime contra o patrimônio no âmbito da Internet, suas peculiaridades e controvérsias à luz do Código Penal de 1940. In: Âmbito Jurídico, Rio Grande, XV, n. 104, set 2012. Disponível em: <http://ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12231&revista_caderno=17>. Acesso em: 15 out. 2014

POZZEBON, Rafaela. Diferença entre: vírus, spam, spyware, worm, phishing, botnet, rootkit. Disponível em: < http://www.oficinadanet.com.br/post/12991-diferenca-entre-virus-spam-spyware-worm-phishing-botnet-rootkit >. Acesso em: 25 set. 2014

PROJETABRASIL. Ddisponível em: <http://www.protejabrasil.com.br/br/>. Acesso em 10 out. 2014

ROSSINI, Augusto. Informática, telemática e direito penal. São Paulo, Memória Jurídica Editora, 2004.

TURBAN, E.; RAINER JR, R. K; POTTER, R.E. **Introdução a Sistemas de Informação: uma abordagem gerencial:** Rio de Janeiro: Elsevier, 2007.

WENDT, E. ; BARRETO, A. G. **Inteligência Digital: foco nas fontes abertas como ferramentas para produção de provas e conhecimentos de inteligência policial**.: Rio de Janeiro: Brasport, 2013.